Homework 9
1.264, Fall 2013
Security
Due: Wednesday, November 27

A series of security questions have been raised as you develop the aircraft parts system. Please answer each of the following questions in one page or less.

1. You have concluded an agreement for very close supply chain integration with ten key customers. You will hold a Web meeting with the others to discuss how to integrate access between supply chain functions. Each of the 11 parties will be able to log into all other ERP systems to perform basic supply chain functions such as order placement, checking shipment status, checking inventory, and invoice submission. Each party can only access a restricted portion of each ERP system. Each party has a different ERP system; each ERP has both Web services and Web page interfaces. You must develop a proposed approach for security.

   Recommend a method for the parties to log into each system. Options include usernames/passwords, SSL certificates (for server and client), and/or Kerberos tickets. Briefly describe the pros and cons of each approach, and the basis for the one you recommend. Assume all 11 ERP systems support Kerberos, SSL and username/password security. Briefly discuss who administers each option: is it centralized over all 11 ERPs, or decentralized?

2. Using the notation in Anderson, define the protocol that is used by customer vehicles transporting materials out of your facilities. Assume:
   a. Drivers have IDs with personally identifying information
   b. Drivers have a smartcard issued by the aircraft parts company to the driver's carrier/employer that is used to open the gate to the parts distribution center. The card uses the same protocol as in the lecture 26 notes: T -> G : T, $\{T, N\}_{KT}$
   c. For each shipment, inbound or outbound, the freight bill number is provided electronically by the parts distributor to the carrier via a secure Web service using RSA encryption. The carrier provides it to the driver via email before the driver arrives at the distribution center.
   d. The driver taps his or her smart card at the gate
   e. The gate writes an access code to the smart card, which will be used at the loading door at your facility. This is encrypted with KT.
   f. The gate prompts the driver to key in the freight bill number at a touchpad at the gate.
   g. The gate will open after a valid smart card is tapped and a valid freight bill number is entered.

   This may or may not be a good protocol.

   a. Define all the principals and variables in the protocol
   b. Define the protocol using the same notation used in lecture (e.g., T->G: T, $\{T, N\}_{KT.}$ Your protocol will have steps corresponding to the description above.

3. List three potential flaws in the protocol in question 2. Then describe one or more attacks that use these flaws, individually or in combination, to enter the facility improperly and/or steal a truck and its contents. Assume your attacker has substantial resources.

    a. List the flaws
    b. Describe one or more attacks

4. Your security plan has the following elements:
    a. Physical barriers at access points and surrounding the facility: fences, building doors and gates for vehicle access.
    b. Access control for employees and visitors, based on smart cards, providing access through gates and doors, as described in question 2 above.
    c. Video monitoring of perimeter of distribution center, at fences, gates and outside doors.
    d. Inspection of inbound and outbound materials at the loading dock.
    e. Security staff to issue and monitor cards, monitor video, and periodically patrol the facility.
    f. Kerberos or SSL/certificate security for your ERP systems, Web servers and databases.

    Develop 5 use cases in which an intruder can gain access to the distribution center, including transportation vehicles and the facility, or its data, including financial or payment data. Make reasonable assumptions about the implementation of the aircraft parts distributor's security plan; you may specify the details as you wish, as part of your scenarios. Assume your attacker has substantial resources and is seeking financial gain. Try to develop the five most likely use cases. You may either draw a use case diagram, or just list the scenarios.

5. The parts distributor has decided to issue smart cards to each driver for each of the transportation carriers that serve it, an improvement over its current system. The parts distributor has also remedied the other flaws in the current protocol that you have pointed out above. The new smart card and the readers associated with it also have biometric capabilities. Driver fingerprints, iris scans and other features may be used.

    Read Anderson chapter 15 on biometrics, and:
    a. Recommend what, if any, biometric methods should be added to the smart card.
    b. Assess, briefly, what level of security they add

6. **Extra credit (20% of homework).** The parts distributor wishes to improve the safety of the shipments it makes and receives, and requires the use of tachographs and truck speed limiters. Read Anderson section 12.3 and:
    a. Recommend what, if any, methods should be added
    b. Assess, briefly, what level of safety they add

Hand in a Word document with your answers.

1.264J / ESD.264J Database, Internet, and Systems Integration Technologies
Fall 2013